RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-R02

Automate or Die!

How to Scale and Evolve to Fix Our Broken Industry

Ben Tomhave

Security Architect
K12
@falconsview

AUTOMATION IS THE SINGLE MOST IMPORTANT CHARACTERISTIC OF TECHNOLOGICAL ADVANCEMENT

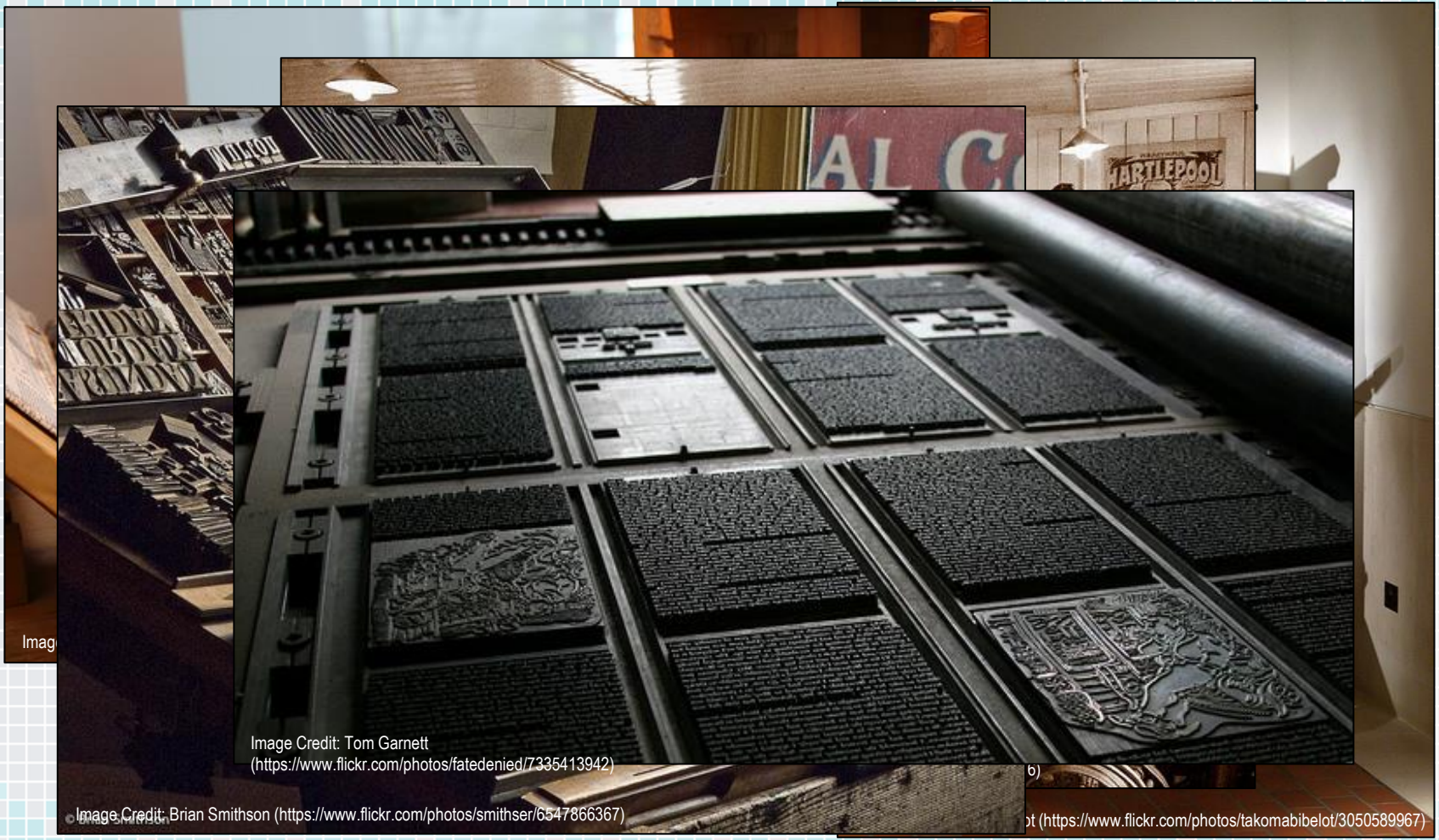


Image Credit: Tom Garnett (https://www.flickr.com/photos/fatedenied/7335413942)

Image Credit: Brian Smithson (https://www.flickr.com/photos/smithser/6547866367)

Image Credit: Steve Jurvetson (https://www.flickr.com/photos/jurvetson/6858583426)

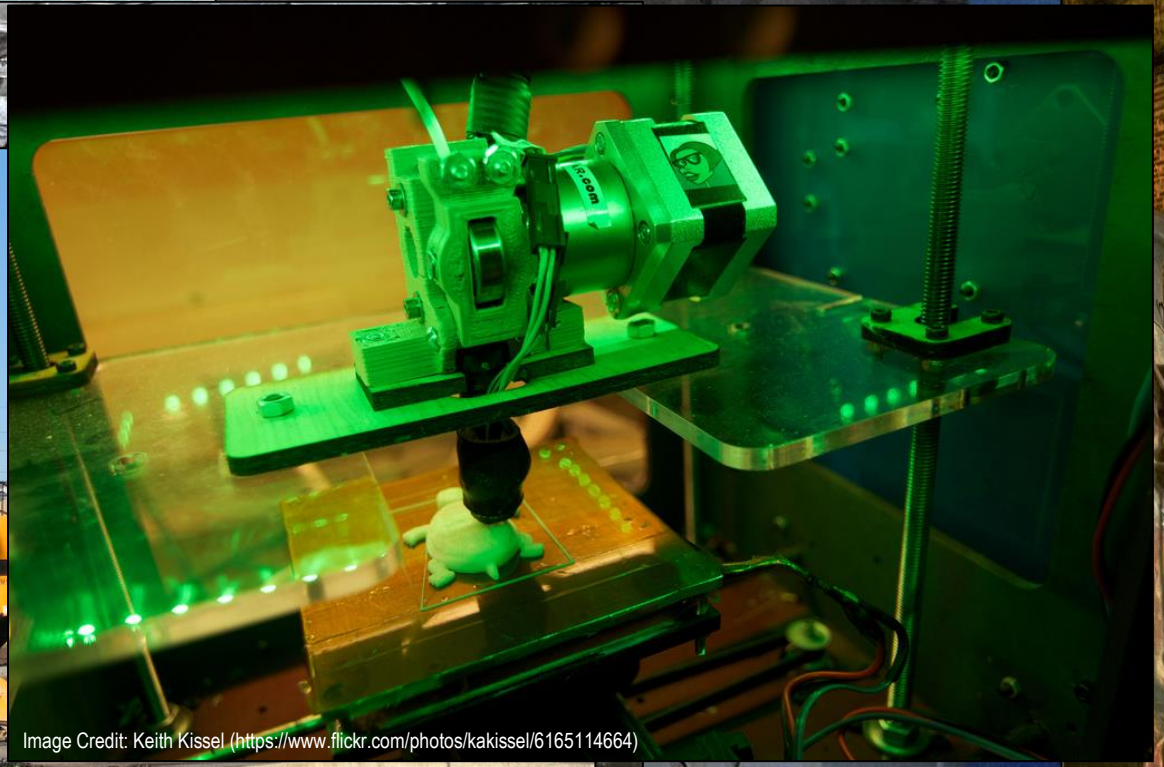


Image Credit: Keith Kissel (https://www.flickr.com/photos/kakissel/6165114664)

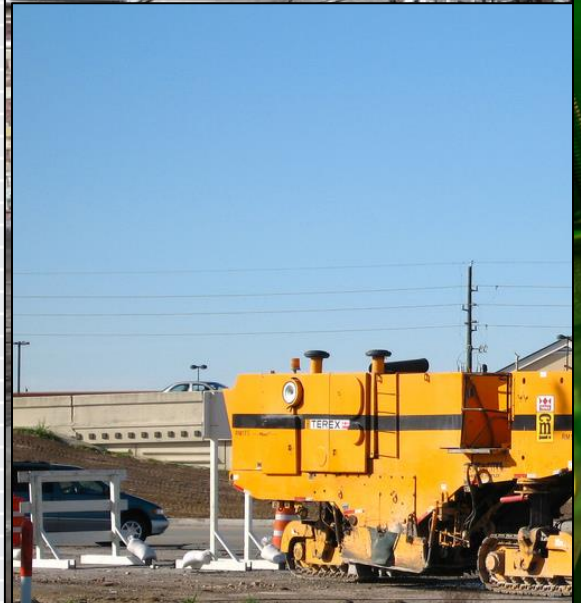


Image Credit: Bill Jacobus (https://www.flickr.com/photos/billjacobus1/115786818)

Image Credit: Forsaken Fotos (https://www.flickr.com/photos/55229469@N07/15565227021)

And the list goes on…

- Mass transportation…
- Communication advances…
  - Telegraph
  - Radio
  - Telephone
  - Satellites
  - Television
  - The Internet!
  - Mobile Devices
- Wearables / IoT

Image Credit: Daniel Rehn (https://www.flickr.com/photos/daniel-rehn/9510955960/)

Convinced Yet? ☺

In the Words of Dr. Dan Geer…

"**One can only conclude that replacing some part of the human cybersecurity worker's job description with automation is necessary.** If the threat space is expanding by X to the Y, then the defense has to arm up accordingly. **An accelerating share of the total cybersecurity responsibility will have to be automated**, will have to be turned over to machines."

"People in the Loop: Are They a Failsafe or a Liability?" (8 February 2012)
http://geer.tinho.net/geer.suitsandspooks.8ii12.txt

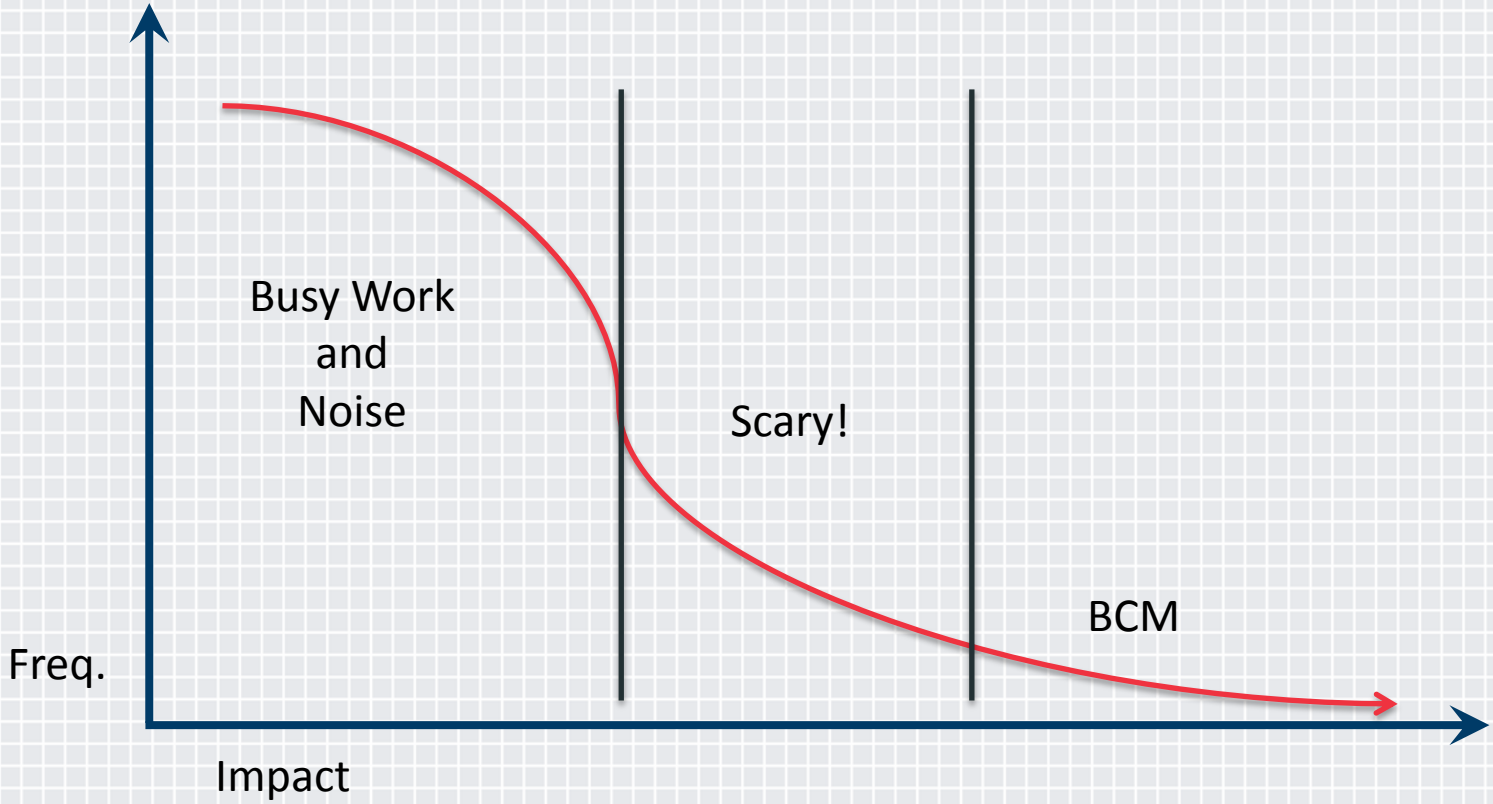
Or Maybe Verizon DBIR 2015?

"It may not be obvious at first glance, but **the common denominator across the top four patterns - accounting for nearly 90% of all incidents - is people**. Whether it's goofing up, getting infected, behaving badly, or losing stuff, most incidents fall in the PEBKAC and ID-10T über-patterns." (p32)

Verizon Data Breach Investigation Report 2015
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf

Problem Statement

"A perfection of means, and confusion of aims, seems to be our main problem." –Albert Einstein


Busy Work
and
Noise
Scary!
BCM
Freq.
Impact

What to do?

Automate!

For Scalability & Resiliency

For Better Quality / Less Errors

For Agility & Responsiveness

Analytics, AI, & Automation

- Current State
  - Just starting to become mainstream…
  - See: DevOps
  - Infosec needs to catch up to ops & dev…
- Many dependencies
- What's the motivation?
  - All these breaches, yet life goes on…
  - Are we trading one "risk" for another?
  - $$$ is *not* insignificant!

Caveat / Warning:

"The question is under what circumstances that we still control can that turning over be a good thing? **How can we put a human back into the loop such that that human *is* a failsafe.**"

(Dr. Geer, also Feb 2012)

Benefits of an Automated Future

Personal Life

- Transparent federated authentication & high-assurance ID
  - Goodbye card fraud
  - Hello "easier life" - greatly reduces friction (shopping, travel (TSA), legal matters, financial matters, hiring, etc, etc, etc)
  - Privacy sidebar: who has control: you or an entity (corp/gov)?
- Wearables lead to real-time medical tracking and alerts
  - *“Grandma, we see you’ve fallen, can you get up?”*
- Revisiting the long tail...
  - Or, social clustering and the reinforcement of confirmation bias...

Benefits of an Automated Future

Business Life

- Transparent federated authN, high-assurance ID
- Self-defending networks? e.g., NAC+DDoS Mitigation+IPS+???
- Knock down high frequency noise
- Application security testing automation
- Address low-end skills gaps through AI+automation

Key Objective: Scaling while minimizing human error

Targets for Automation: A Few Examples

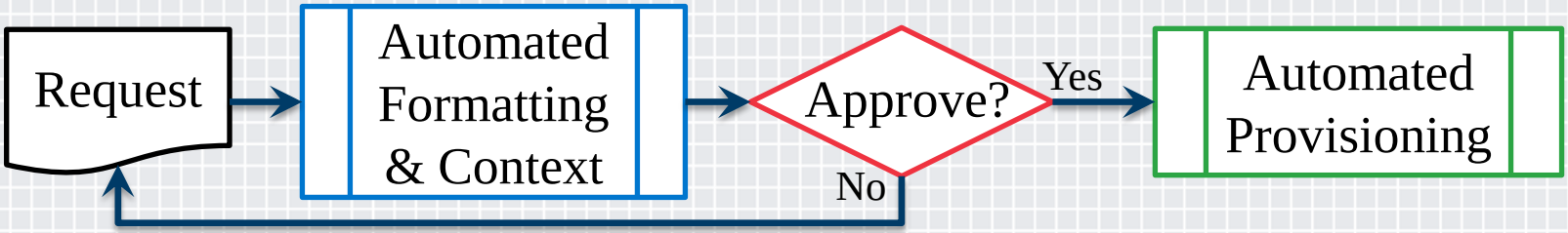
- Internal DNS updates
- Firewall rule deployments
- Access deployments & terminations
- Account reconciliation
- HR/Legal holds
- Incident context for investigations
- Application security

Pick “low risk” activities that are easily scripted.

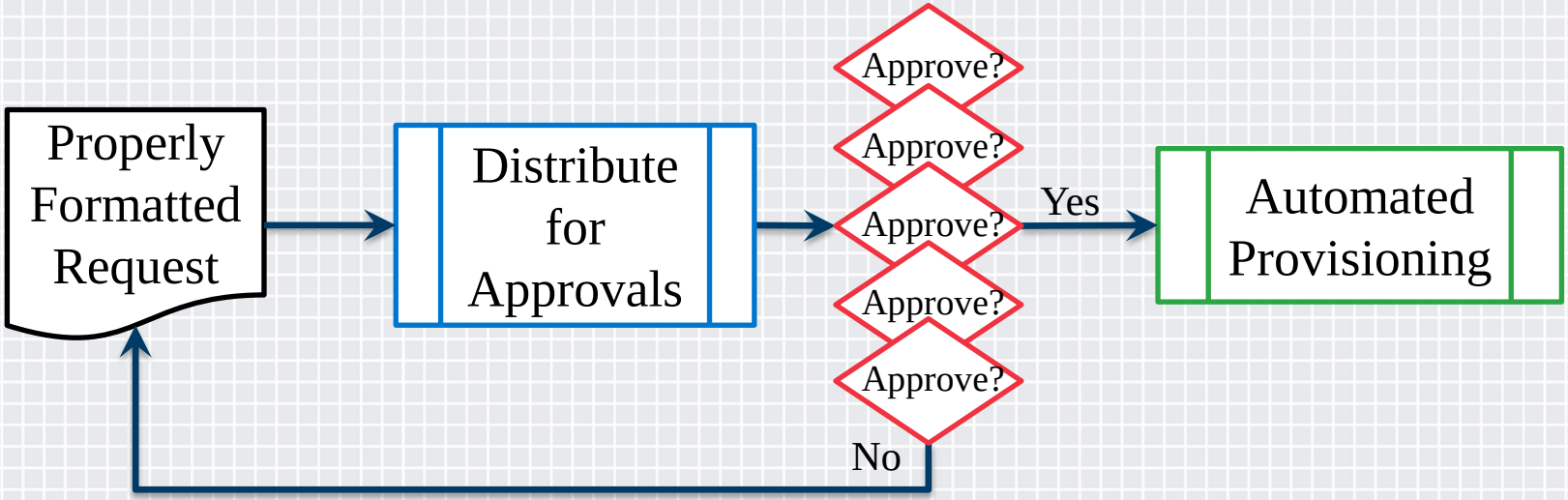
Note: Yes, we already see some of these things being automated today!

Automated Deployment

- Internal DNS Update
- Firewall Rule Deployment

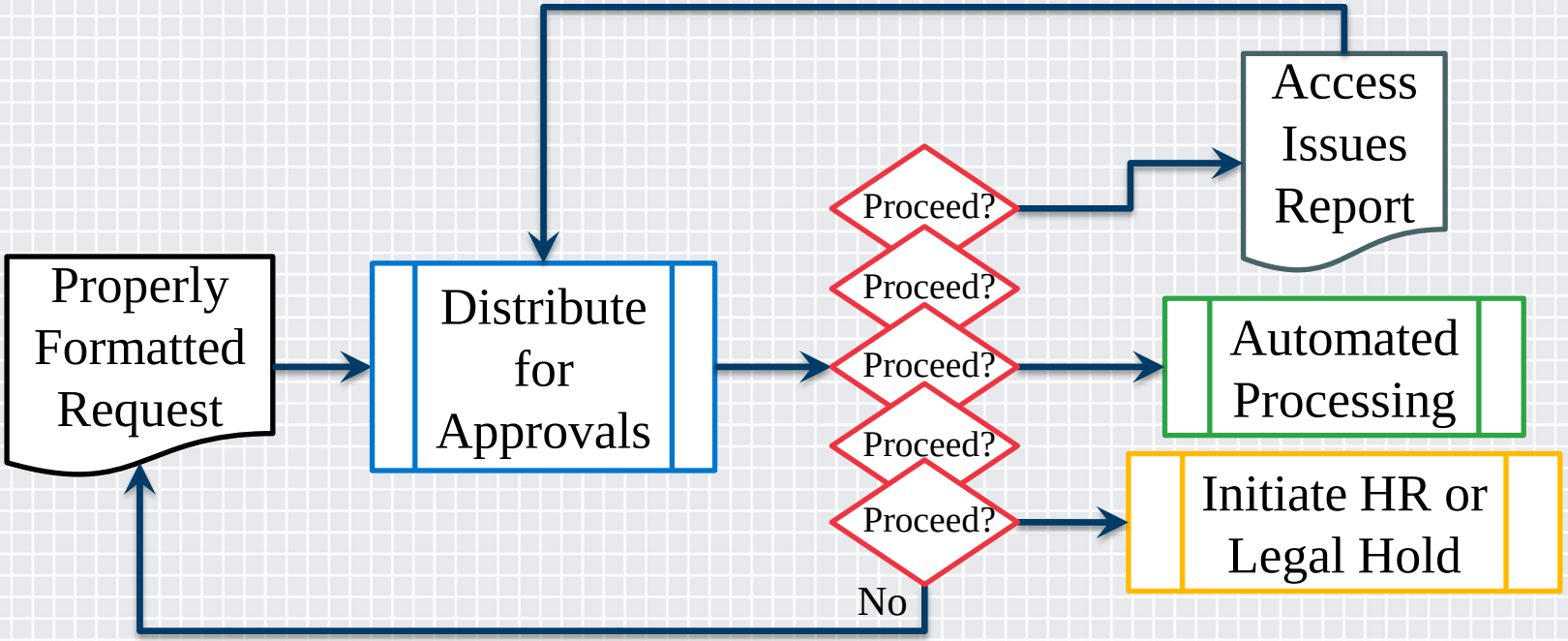


Access Deployment



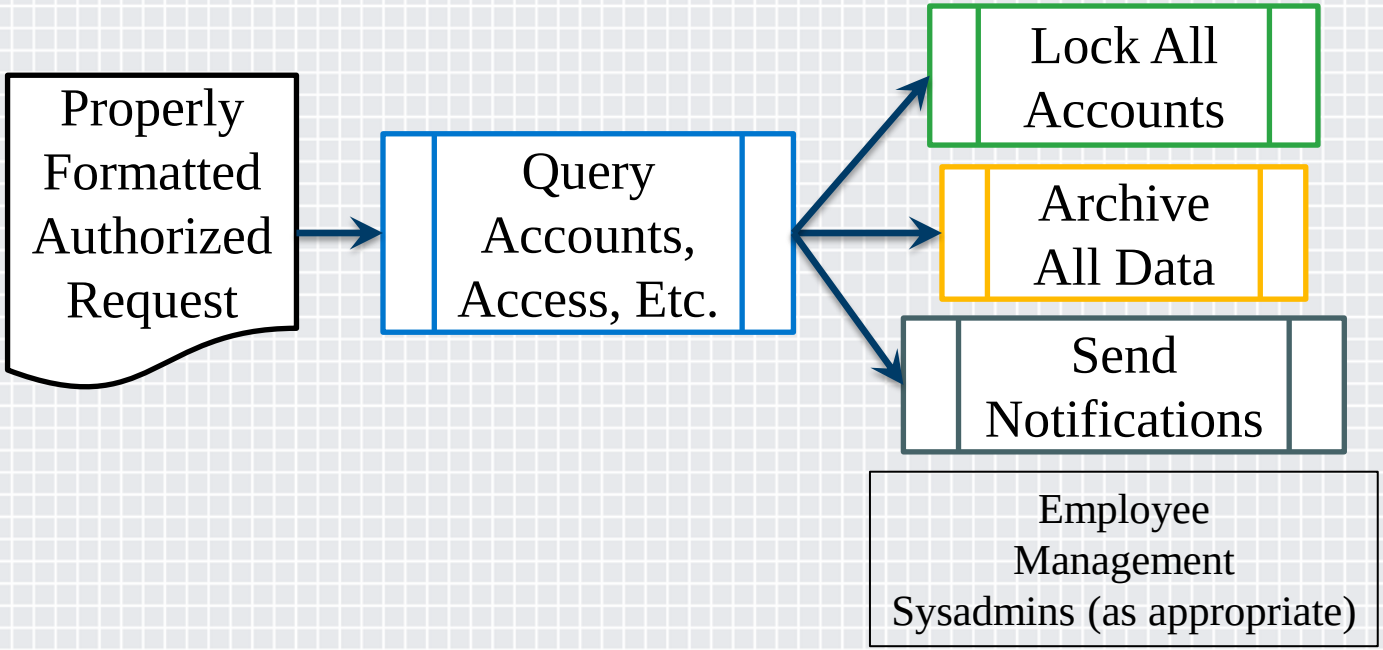
Assumption: A system of record exists!

Access Term./Acct. Reconciliation



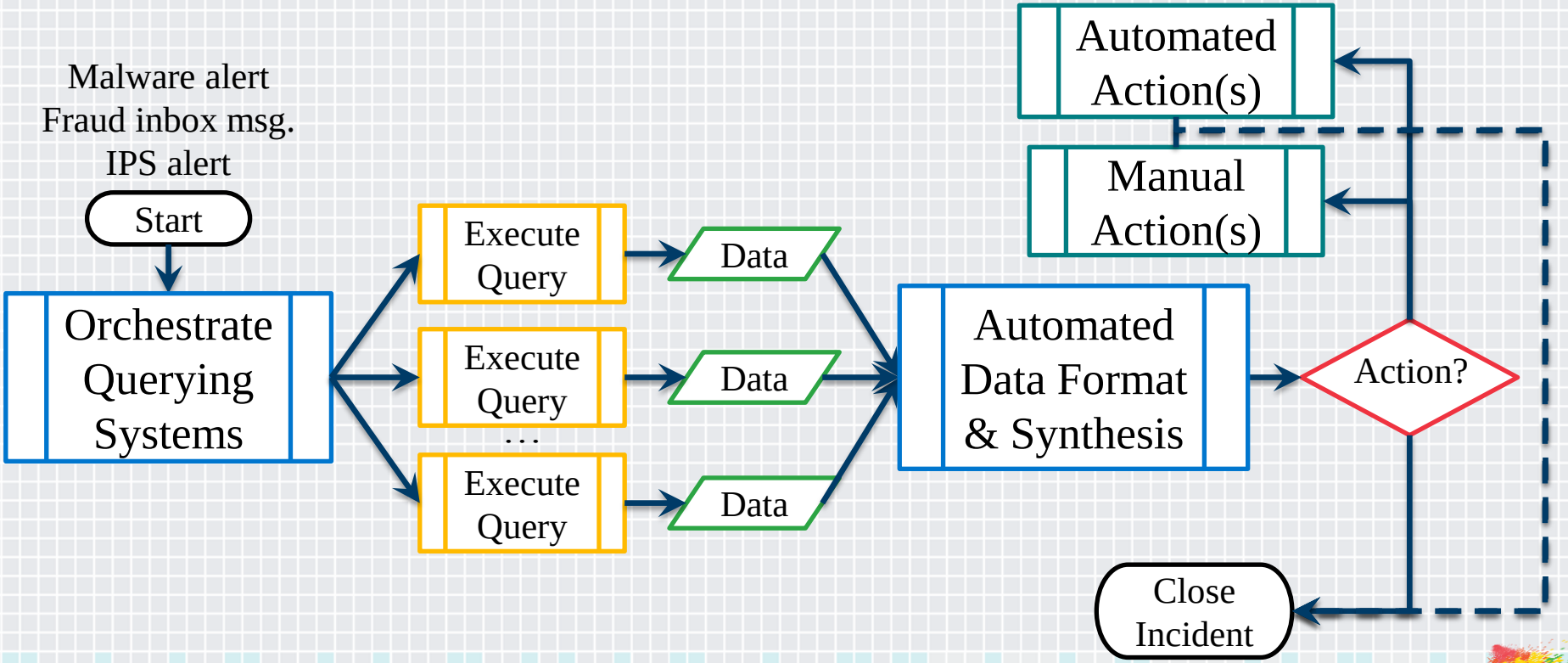
Assumption: A system of record exists!

HR/Legal Holds

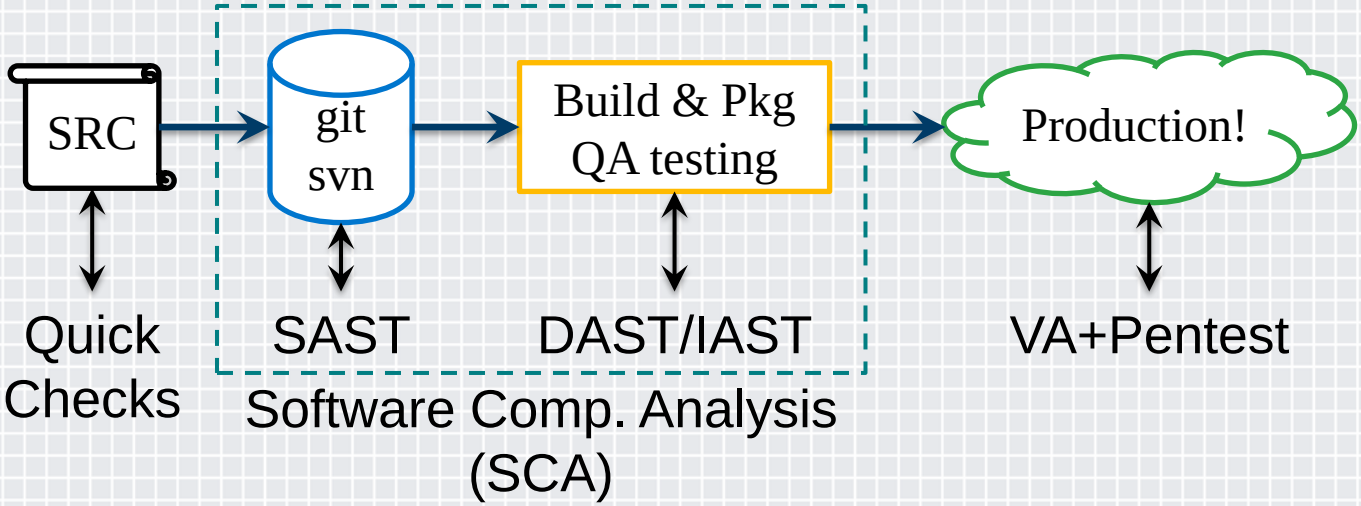


Assumption: A system of record exists!

Incident Support



Application Security



***Note*: All results feed directly back into standard issue management!**

Things to Consider…

- Are you copying data from one system to paste into another?
- Are there highly repetitive tasks that could be automated with basic data input?
- Automation is *not* the absence of manual intervention, but the facilitation of *smarter* manual involvement *only as needed*!

With automation comes the impetus for positive resource utilization shifts. Now you can survive with a couple high-value resources instead of entire teams of them. Automation not only improves scalability, but it also improves quality by reducing human error!

What Tools Can You Use?

This is just a quick sampling… literally dozens more, FOSS or commercial!

csg INVOTAS

puppet labs

CHEF

palerra

Jenkins

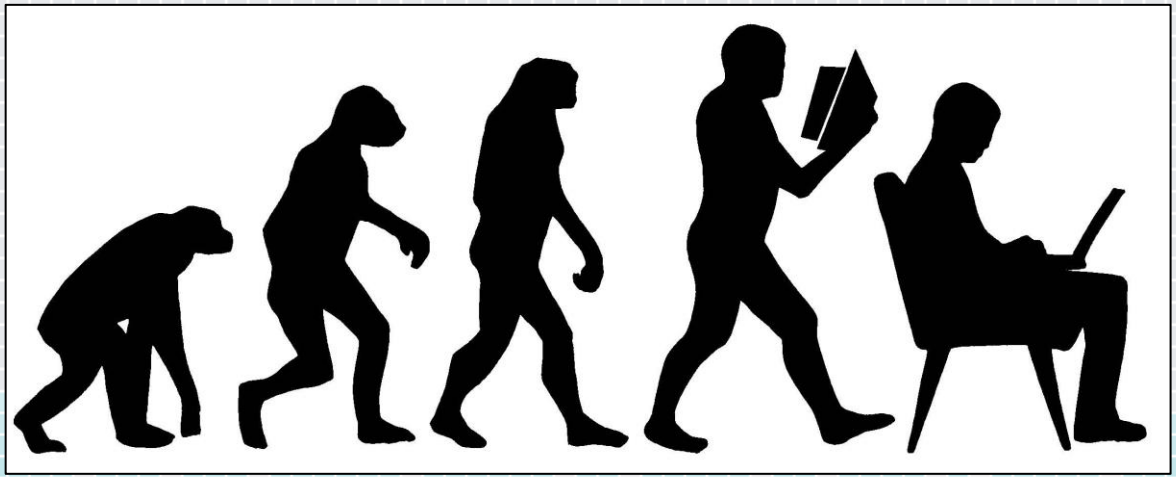
Nagios®

servicenow

SALTSTACK

The Evolutionary Imperative

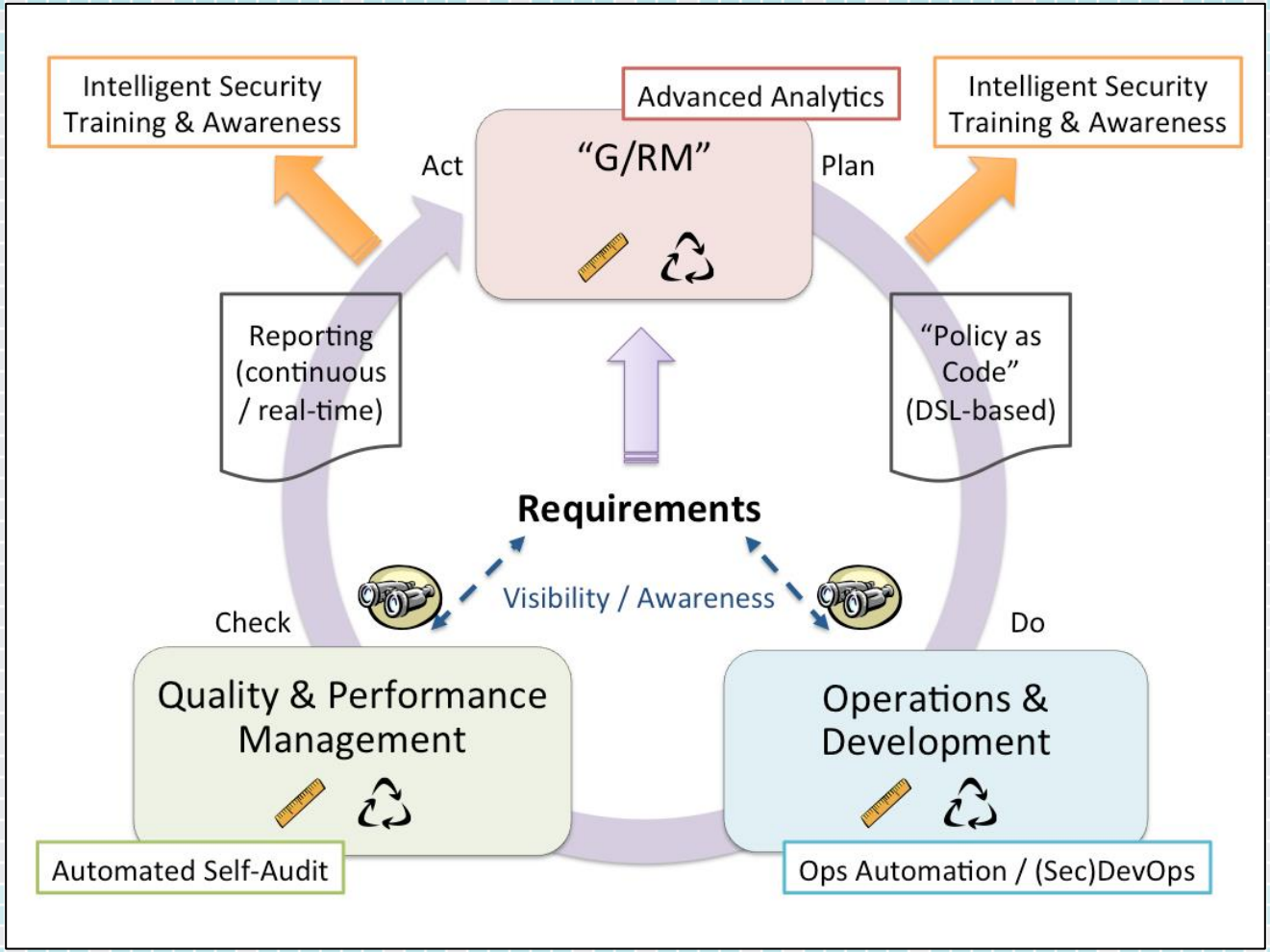
- We ***must*** evolve, or we ***will*** die.
- Evolution is in response to survivalist intuition.
- Choose to survive!



Survival Tips

- Shift risk management mindset → architecting for resiliency
  - DevOps + "all the world's a cloud" + IRM
  - Embrace the benefits of utility compute power
  - Automate where possible, shift resources to important things!
- Empower users
  - The secure choice should be the easy choice
  - Don't be a barrier!
  - Incentivize good decisions
- **Remember**: It's not just about achieving an ideal!


My Grand Vision



Intelligent Security Training & Awareness
Advanced Analytics
Intelligent Security Training & Awareness
Act
"G/RM"
Plan
Reporting (continuous / real-time)
"Policy as Code" (DSL-based)
Requirements
Visibility / Awareness
Check
Do
Quality & Performance Management
Operations & Development
Automated Self-Audit
Ops Automation / (Sec)DevOps

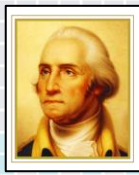
Apply What You Have Learned Today

- Now:
  - Identify targets for automation
  - Begin building foundational tool chains (e.g., ops orchestration)
  - Establish key repositories (e.g., IDM system of record)
- Soon:
  - Implement & deploy!
- Long-term:
  - Automate first, manually intervene second (humans as failsafe)

THANK YOU!

Ben Tomhave • @falconsview • www.secureconsulting.net

LUTHER COLLEGE



THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

k12

ISSA
Information Systems Security Association

CISSP®